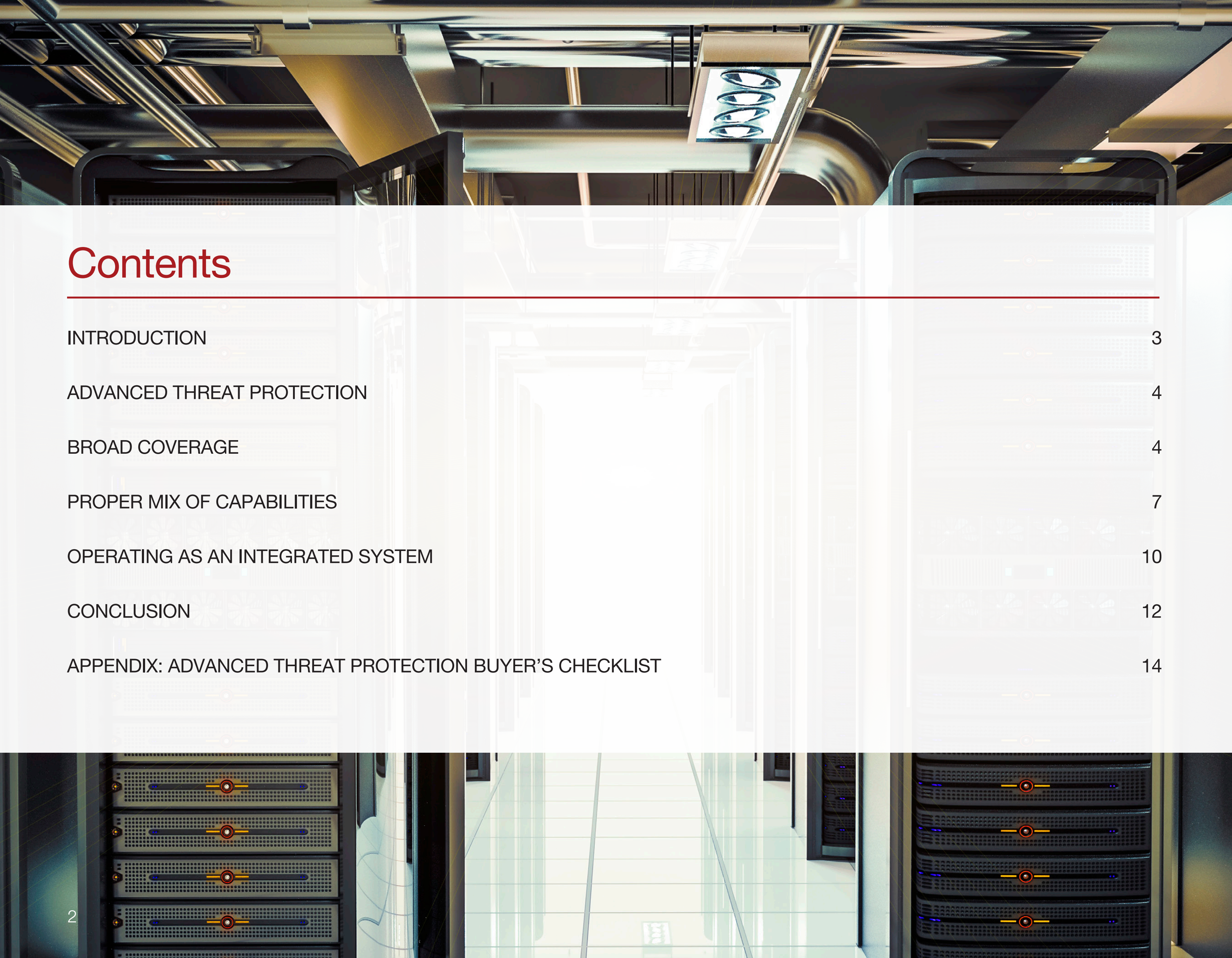
FORTINET®

# Advanced Threat Protection Buyer's Guide

## GUIDANCE TO ADVANCE YOUR ORGANIZATION'S SECURITY POSTURE



# Contents

# Introduction

The volume and impact of data breaches stemming from increasingly sophisticated attacks continues to increase. In many cases, such attacks are specially crafted and tested to bypass traditional security measures and customized to target individual organizations.

To deal with these advanced threats, most security analysts, experts and vendors advocate a combination of improved prevention, new advanced threat detection and incident response. While solutions may sound similar at the surface, differences emerge upon closer investigation.

This guide will help you assess your current and proposed security posture against a baseline set of requirements to ultimately ensure the right solution set for your organization.

# Advanced Threat Protection

While much excitement focuses on new technologies like network sandboxing, there is no single product answer to the challenge of advanced threats. In the report *Best Practices for Detecting and Mitigating Advanced Persistent Threats,*[1] Gartner says, "Information security practitioners must implement specific strategic and tactical best practices to detect and mitigate advanced persistent threats and targeted malware by leveraging both existing and emerging security."

Fortinet agrees and recommends:

1. **Broad coverage** throughout the organization, with
2. The proper mix of **prevention, detection and mitigation,** that
3. **Operates as a cohesive security system** rather than a collection of individual piece parts.

Ensuring that your enterprise security infrastructure addresses all three of these aspects will yield the strongest defense.

## BROAD COVERAGE

Today's enterprise environment is evolving and dynamic, driven largely by mobility, cloud services, encrypted communications and more. This introduces new complexities to ensure the proper degree of security coverage to protect users, systems and data. When assessing and improving your ability to defend against today's sophisticated cyber threats, it is important to take into account the physical location, digital communications and sheer capacity of data to be inspected and protected.

## Physical Locations

Organizations typically start at logical Internet ingress and egress points, which may either be consolidated in data centers or increasingly distributed to local offices—all of which are key check points for security inspection. Additionally, assessing traffic related to sensitive network segments at the core is critical. Beyond that, pushing inspection to endpoints that may be exposed to threats outside the network and to applications and data that may reside in public cloud infrastructures should also be considered. While it can be challenging to apply the same combination of security technologies everywhere, smaller protection coverage increases the risk of blind spots that can be exploited and compromised.

## Digital Communications

Analyzing activity from a physical position does not inherently ensure you can inspect all traffic. Generally defined by protocol, organizations need to specify the communications over which security analysis is applied. Web (http) and email (SMTP) are the most common starting points and also the most common attack vectors. According to the *2015 Data Breach Investigations Report*,[2] Verizon ranked web the top exploited access vector followed by email. Also consider inspecting file delivery and storage (by FTP or SMB). Most importantly, don't forget to factor in encrypted protocols. Excluding encrypted traffic can give cybercriminals free entry.

## Performance and Capacity

If not sized correctly, security solutions can get overwhelmed by the volume of packets and activity to analyze. Especially if deployed directly in the production flow, ensure that the products selected have port capacity to accept packets, software performance to keep up with them and execution capacity to analyze the volume of data collected. Dropped packets or overlong queues limit coverage even when physical position and digital communications are established and supported.

### Expert Tip #1

As an organization’s security model evolves, it is natural to adopt new security components, often from new vendors. For example, many organizations have added mobile device management (MDM) from pure play vendors to address mobility and the multi-device users. Similarly, as workloads have moved to cloud infrastructure, many have added security from start-ups focused on these elastic environments. Unfortunately, this point product approach provides security coverage in an uneven fashion across the evolving enterprise environment. While some elements of security (prevention, detection or mitigation) may be in place everywhere, they may not always be the best or most complete set for the strongest security posture.

## PROPER MIX OF CAPABILITIES

To date, the majority of enterprise security investments have focused on prevention with relatively limited introduction of detection and mitigation components. However, organizations should establish the proper balance across each component set. According to a November 2015 study by Forrester, 87% of organizations surveyed experienced at least one security breach in the past 12 months[3], which demonstrates the importance of detection and mitigation.

### Prevention

A successful prevention capability relies on multiple technologies working together to reduce the attack surface and block threats from entering the network. Such technologies include signatures and heuristics to block malicious code (anti-malware), traffic (intrusion prevention) or applications (application control), reputations to rate Internet sites (web filtering), email senders (email reputation), or IPs (botnet detection) and more. It is important to prevent as much as you can in order to reduce the expensive and time-consuming analysis and effort of advanced threat detection and mitigation. Upgrading your "traditional" threat prevention products to obtain more effective and proactive prevention can greatly improve your ability to defend against today's sophisticated threats. Closely assess your existing network, web, email and endpoint security to see how well it is or is not doing. And consider adding newer threat prevention components, such as web application firewalls, if they are not already in place.

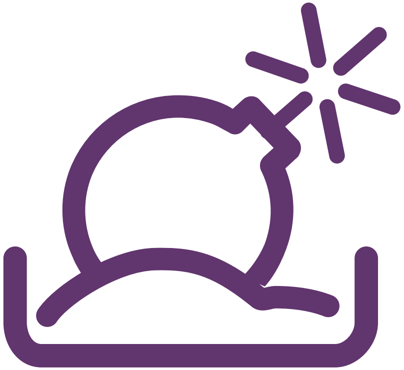
of organizations experienced at least **one security breach in the past 12 months**

## Detection

There are many emerging technologies available to help identify previously unknown threats that bypass prevention measures. One of the most popular and important approaches today is network sandboxing. According to a Forrester study, *Sandbox Technology: Building an Effective Breach Detection and Response Strategy* [4], 87% of experienced security pros reported that sandboxes provide information important in detecting advanced threats. There are also many other techniques that are worth consideration—from dynamic client reputations to network behavior analysis to big data analytics and more. While your organization may not yet be ready for some of these newer technologies, it’s relevant to recognize that the important one of today was preceded by a critical one of yesterday and will be followed by another in the future. This simply parallels the evolution of the threat landscape.

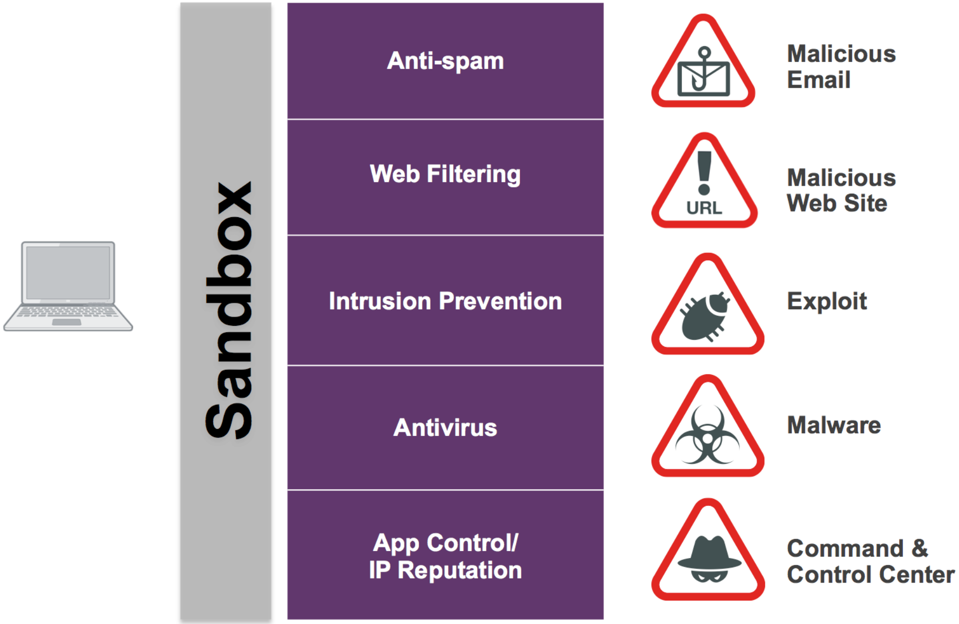
## Mitigation

Of course detection of attacks in progress is of limited value without a corresponding response to mitigate their impacts and avoid a major breach. Organizations must ensure that their detection systems provide appropriate information to enable an effective response. Likewise, responders must have the proper process and tools in place to ensure swift mitigation. Forensic tools, supporting services and even integrations with your existing threat prevention products have a role to play in this effort. The more assisted or automated your response process, the more effective the mitigation effort.



**87% of pros**

reported that sandboxes provide information important in detecting advanced threats

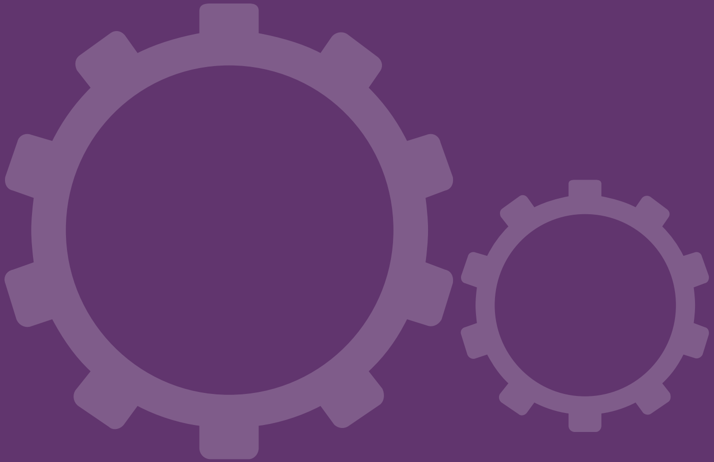


## Expert Tip #2

One of the best ways to assess effectiveness is to utilize independent real-world comparative tests. Although these environments are not exactly the same as yours, they have the benefit of ensuring a large sample set of advanced malware that compares products on equal footing. NSS Labs, Virus Bulletin and AV Comparatives are reputable test houses with transparent test methodologies and recurring comparative test cycles. Depending on how broadly you can test within your own environment, that approach may be preferable. It's ideal if you can perform a rigorous on-site comparative test of multiple solutions, at least for critical security components. At minimum, obtaining a credible measure of the effectiveness of each component is important.

# OPERATING AS AN INTEGRATED SYSTEM

Not only having these components at the right places, but also ensuring they work together as a cohesive system to combat advanced threats is critical. Without this there will be too many gaps in your security posture, which can be exploited by cybercriminals to gain a foothold in your network. Devoid of an integrated system, these gaps must be bridged by human intervention and will inherently widen over time. When assessing your security infrastructure as a whole, look specifically at and for integration points, automated or at least assisted actions and common, central intelligence hubs.



## Integration Points

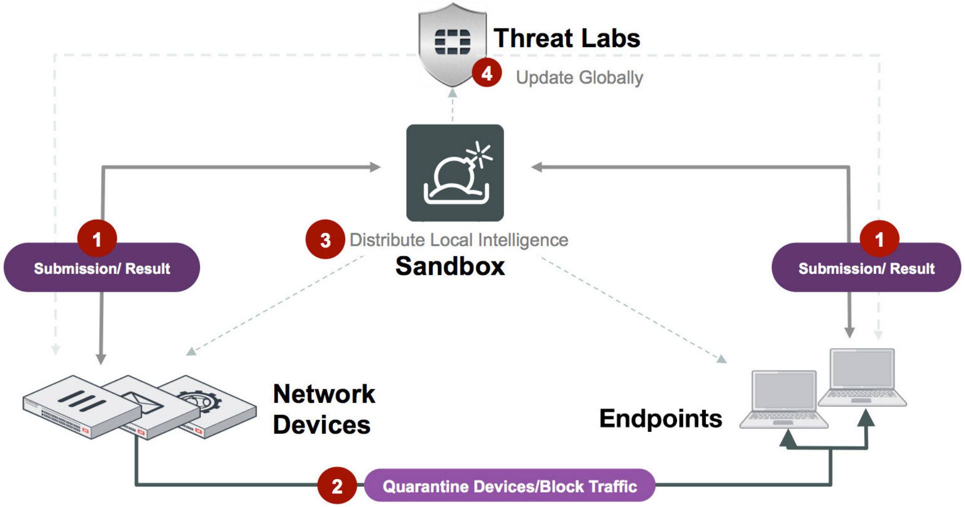
There are multiple ways that information can be exchanged. First, it can be consolidated across physical locations. For example, configurations can be set once for firewalls at the headquarters, branch locations and even cloud infrastructures. Similarly, logs can be consolidated across secure email gateways and firewalls. Second, it can be shared between security elements; for example, prevention products can pass objects to advanced threat detection components for analysis. Similarly, detection products can pass information to response systems to speed mitigation. Third, it can be passed via emerging standard APIs and formats for broader sharing. For example, JSON APIs or STIXX/TAXII standard data structures speed integration more broadly. In the near-term, look for integrations across your security elements until such intelligence sharing standards become the norm.

## Automation

Beyond the simple exchange of information, the ability for actions based on that information to be automated (or at least assisted if a degree of human oversight is desired) is critical. For example, the ability for advanced threat detection to automatically generate threat intelligence updates that are then passed to your threat prevention products for immediate blocking is quite helpful. Similarly, the sharing of indicators of compromise helps speed administrative responses, such as quarantining at risk systems or blocking high risk IP addresses.

## Central Intelligence Hub

Of course the aforementioned are all tactical responses. It is also important to enable strategic responses that result in a constantly improving security posture. This includes the development and broad distribution of proactive prevention intelligence, development of new core security technologies and much more. Ideally the intelligence sharing sharing will happen both locally, directly among your deployed components and globally through an expert threat research Lab.



### Expert Tip #3

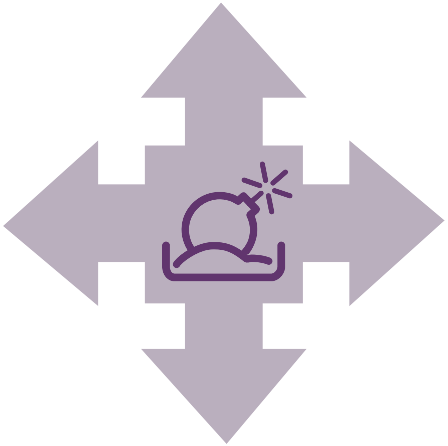
While integration and information sharing can and does take place between vendors, organizations should keep in mind that the tightest integrations, highest degree of automation and fastest sharing of intelligence is most likely to occur among solution sets from a single vendor. That said, just because a set of products is sold by a single vendor there is no guarantee they will integrate, automate or share intelligence with each other. This especially can occur with vendors that routinely expand portfolios through acquisition, so be sure to examine closely to ensure tight product integrations are supported.

# CONCLUSION

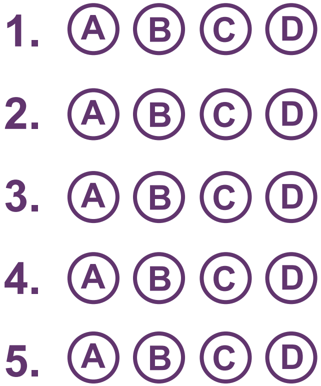
Advanced threats vary in sophistication but many are bypassing traditional defenses, as evidenced by the recurring data breach headlines, industry reports and analyst recommendations. Organizations seeking to improve their defenses against these threats must do more than simply add on the latest security technology "du jour" even if it is an important one. Specifically, Fortinet recommends:

- ✓ Ensuring breadth and depth of coverage across your dynamic organization (from physical to cloud), including the optimal mix of prevention, detection and response for each point of control.
- ✓ Employing rigorous independent testing to assess the effectiveness of each security component in order to prevent as much as possible and quickly detect and respond to previously unknown threats.
- ✓ Moving towards a cohesive security solution that leverages integration, automation and a common intelligence hub (locally and via global research organizations) to close gaps and make cost and effort manageable for the average organization.

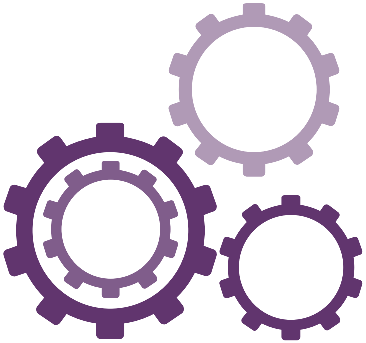
## Breadth and Depth



## Rigorous Testing



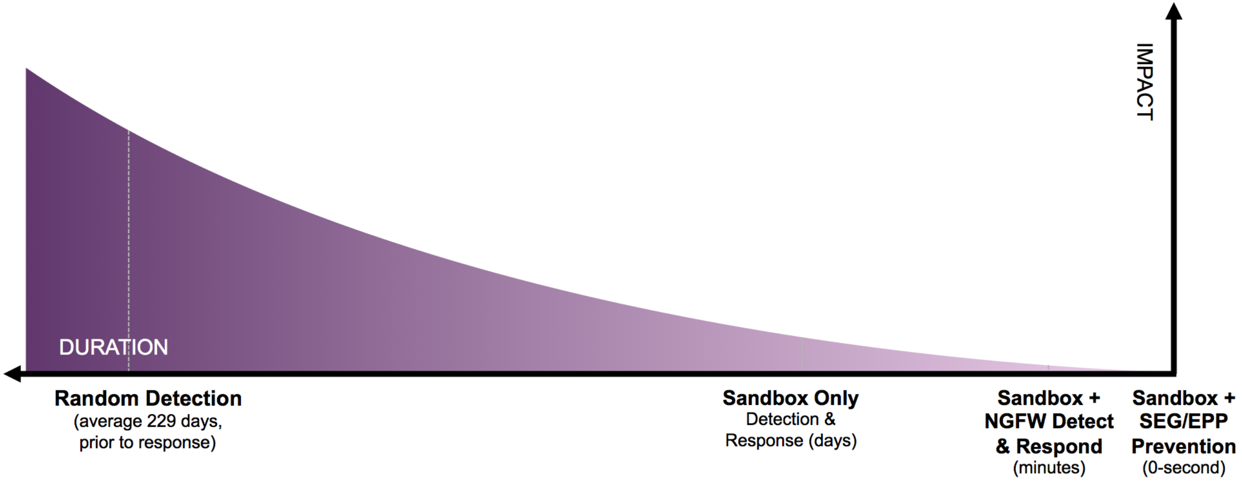
## Cohesive Defense



Organizations are at varied stages in their security maturity model. As a top priority, ensure you have demonstrably effective sandbox analysis. This is critical to protect your organization's most sensitive information, and ideally, it should be applied as broadly throughout your organization as you can afford and manage. Next, prepare to manage the risks your sandbox analysis uncovers with an efficient mitigation response process. A secure email gateway with an integrated sandbox provides the ability to block even the newest targeted email attacks, so offers an excellent early step in your mitigation response efforts. This can either be a supplement to your current email security solution or its replacement.

As opportunities naturally arise to reconsider your network, web application and endpoint security, prioritize the evaluation of products that will leverage your initial sandbox investment in order to expand coverage and progress towards a more effective response and cohesive system.

Although your initial sandbox investment may not include any threat prevention or mitigation components, given the importance to expand your sandbox integrations over time, your chosen solution should include integration to quality components that you can consider at the right time in the future. Without this capability, your organization will be stuck with a patchwork of security products that leaves gaps and requires heavy administrative and response effort.



# Appendix: Advanced Threat Protection Buyer's Checklist

The checklist below will help you assess your current and proposed security posture with a look at your environment coverage, mix of security technologies and integration capabilities. The end result will provide you with a baseline set of requirements to ultimately ensure the right solution set for your organization.

## I. EVALUATE ENVIRONMENT COVERAGE

□ Determine the physical locations you want to cover, such as network ingress/egress/internal points, central email and file systems, mobile endpoints and cloud workloads.

□ Decide which protocols you want to inspect at each of those points (e.g., http, SMTP, SMB and more, including encrypted versions).

□ Assess the capacity that is required (e.g., 1 G, 10 G, 40 G Ports and/or 1 Gbps, 4 Gbps, 10Gbps or more, plus the number of objects per time period).

□ Evaluate or review the most recent independent comparative tests that cover sandbox and related technologies to understand how they performed. Refer to test houses such as NSS Labs, Virus Bulletin, AV Comparatives and ICSA Labs.

These steps will help you properly size the necessary deployment and quickly see past loss leader, feature-limited point products that lead you down an expensive and unsustainable path as well as vendor marketing hype that hides insufficient effectiveness.

## II. DETERMINE YOUR MIX OF SECURITY TECHNOLOGIES

□ Understand what analysis techniques are utilized for prevention by location and protocol and ensure you have more advanced techniques in place to block as much as possible (e.g., signatures, heuristics, reputations, emulation and decryption).

□ Learn what analysis techniques are used to provide advanced threat detection by location and protocol, including sandboxing, behavioral analysis and big data analytics.

□ Identify the mitigation processes and tools you have in place to respond to incidents. This may include your response team, outside services, forensic tools and integration, as well as automated response between products.

□ Identify the methods used to assess the effectiveness of your threat prevention, detection and mitigation (e.g., regular penetration tests, tracking production effectiveness, time of purchase PoC and independent test reports).

These steps will help you focus and balance your investment for maximum results across each of the three elements. It is important that you don't overlook ways to prevent more advanced threats before time-consuming detection and response are required. However, overlooking detection and relying solely on prevention is also folly as we have seen these past few years. Likewise, prevention and detection investments without the ability to respond will not effectively reduce your security risk.

## III. DEGREE OF SYSTEM-LEVEL OPERATION

□ Identify which prevention components integrate detection elements with each other (e.g., firewall integration across branch, HQ, core, cloud; email and web security, end point protection, web application firewall, SIEM, log management and others).

□ Define how advanced threat detection components provide information for response (e.g., dashboards and reports, export data via APIs, established integrations to pass data and automatic signatures).

□ Understand which assisted or automated responses can be taken by in-place components (e.g., quarantine devices, block sources or remove files).

□ Identify how many central intelligence hubs, local threat exchanges and/or global research labs are required.

This will determine the degree to which all of your prevention, detection and mitigation elements, however good on their own, function efficiently and effectively as a cohesive security solution.

# Rating the Strength of Advanced Threat Protection

To assess the general strength of your organization's defense against today's sophisticated threats, gauge the number of prevention technologies in place, measures to detect and mitigate advanced threats that may skip through, and integration points between all of these aspects.

A wide range of prevention with few advanced detection or mitigation components leaves organizations exceptionally vulnerable. Even many individual components will still leave gaps. See where you stand today and make informed choices to move toward an integrated system of prevention, detection and mitigation.

## PREVENTION COMPONENTS

- □ Branch Firewall
- □ HQ Firewall
- □ Core Firewall
- □ Cloud Firewall
- □ Secure Email Gateway
- □ Secure Web Gateway
- □ Web Application Firewall
- □ Endpoint Protection
- □ Other

## DETECTION COMPONENTS

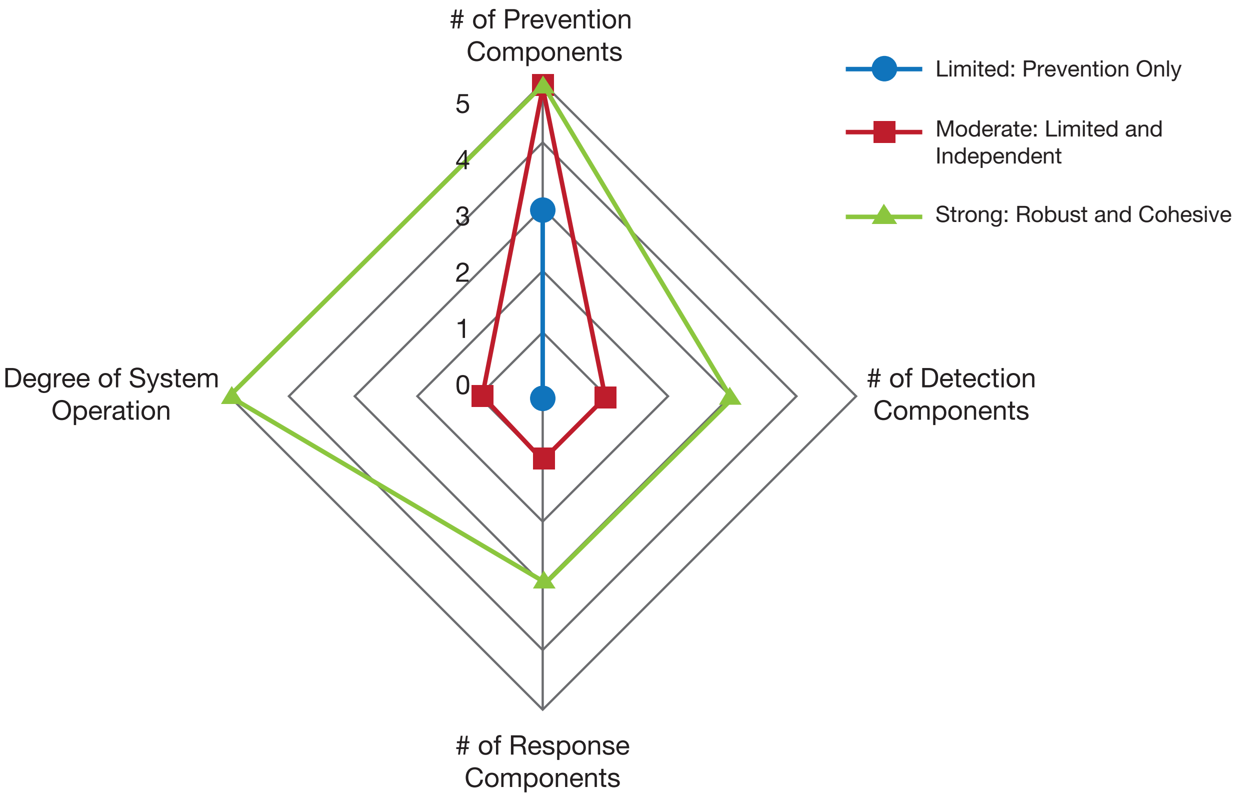
- □ Network Behavior
- □ Network Forensics
- □ Endpoint Behavior
- □ Sandbox
- □ Big Data
- □ Other

## RESPONSE COMPONENTS

- □ Response Services
- □ Endpoint Forensics
- □ Automation

## INTEGRATION POINTS

- □ Firewall and Advanced Threat Detection
- □ Secure Email Gateway and Advanced Threat Detection
- □ Secure Web Gateway and Advanced Threat Detection
- □ Web Application Firewall and Advanced Threat Detection
- □ Endpoint Protection and Advanced Threat Detection



[1] https://www.gartner.com/doc/3043819/best-practices-detecting-mitigating-advanced

[2] http://www.verizonenterprise.com/DBIR/2015/

[3] http://www.fortinet.com/resource_center/analyst_reports/best-defense-next-generation-firewalls.html

[4] http://www.fortinet.com/resource_center/analyst_reports/sandbox-technology-breach-detection-response-strategy.html

FORTINET®

v1.0 02.01.16